

## **REMARKS**

In response to the above-identified Office Action, Applicant seeks reconsideration of the application. In this response, no claims have been canceled, no claims have been added, and no claims have been amended. Accordingly, Claims 1-26 are pending.

### **I. 35 U.S.C. § 112**

Claim 3 has been rejected for failure to provide sufficient antecedent basis for “the media key” limitation in line 22. Applicant notes that the antecedent bases for “the media key” can be found in line 20. Specifically, Claim 3 recites the encryption subsystem that comprises “a processing logic ... to compute a media key” and “a one-way function to generate the encryption bus key based on the media key ...”. It is therefore respectfully submitted that the rejection under U.S.C. 112 be withdrawn.

### **II. 35 U.S.C. § 103**

The Examiner has rejected Claims 1-26 under 35 U.S.C. §103(a) as being unpatentable over Natsume et al., “DVD Content Scramble System, June 1997, National Technical Report, Vol. 43, No. 3, pp. 338-342 (Natsume) in view of U.S. Patent No. 6,272,225 B1 issued to Miyauchi et al. (Miyauchi). Applicant respectfully traverses this rejection.

The system claimed in Claim 1 requires deriving an encryption bus key based on [1] a nonce generated by a number generator, [2] at least a portion of a key distribution data block and [3] at least one device key assigned to an encryption subsystem. The system claimed in Claim 1 further requires that the encryption bus key is used to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus.

Applicant respectfully submits that Claim 1 is not obvious over Natsume in view of Miyauchi. Particularly, Applicant submits that the combination of Natsume and Miyauchi fails to teach deriving an encryption bus key based on [1] a nonce generated by a number generator, [2] at least a portion of a key distribution data block and [3] at least one device key assigned to an encryption subsystem. Furthermore, Applicant submits that neither Natsume nor Miyauchi teaches or suggests using an encryption bus key, which has been derived based on the above-mentioned elements or values, to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus.

In rejecting Claim 1, the Examiner asserts that “Natsume discloses a system comprising: an encryption subsystem [see figure 3] to encrypt data accessed from a storage medium containing a key distribution data block [i.e., encrypted disc key set 12, see figure 2] using an encryption bus key (i.e. title key) prior to transmitting the encrypted data [see page 8 lines 18-21] via a data bus (i.e. PC bus 7, see figure 5). The Examiner’s analysis of Claim 1 is believed to be inaccurate. Particularly, in rejecting Claim 1, the Examiner equates what is shown in figure 3 of Natsume as an encryption subsystem to encrypt data accessed from a storage medium. However, figure 3 of Natsume in no way teaches or suggests an encryption subsystem to encrypt data accessed from a storage medium. Instead, figure 3 of Natsume shows a descrambling system for descrambling scrambled AV data stored on a storage medium. Additionally, in rejecting Claim 1, the Examiner equates a “title key” of Natsume as an encryption bus key as set forth in Claim 1. However, the “title key” taught by Natsume does not serve to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus as set forth in Claim 1. Rather, Natsume discloses that the “title key” is used to descramble scrambled AV data on a disc (see page 11, lines 1-3 of Natsume). The “title key” of Natsume may be used to scramble data before storing the data on the disc. However, there is nothing in Natsume that teaches or suggests that the “title key” may be used to encrypt data accessed from a storage medium prior to transmitting the data via a data bus. Accordingly, Applicant respectfully submits that Claim 1 is not obvious over Natsume in view of Miyauchi and requests withdrawal of this rejection.

Analogous arguments and discussion apply to independent Claim 11. Particularly, Applicant respectfully submits that the combination of Natsume and Miyauchi fails to teach or suggest a method comprising: [1] a storage device reading a key distribution data block from a storage medium; [2] the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key; [3] the storage device fetching a nonce generated by a number generator; [4] the storage device combining said nonce with said media key using a one-way function to generate a bus key; [5] the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and [6] the storage device transmitting the encrypted data over a data bus. Accordingly, Applicant respectfully submits that Claim 11 is not obvious over Natsume in view of Miyauchi and requests withdrawal of this rejection.

Analogous arguments and discussion apply to independent Claim 18. Particularly, Applicant respectfully submits that the combination of Natsume and Miyauchi fails to teach or suggest an apparatus comprising: a storage device to access a storage medium containing data and a key distribution data block, the storage device including a processing logic, a one-way function and an encryption logic, wherein the processing logic processes at least a portion of said key distribution data block using a device key assigned to the storage device to compute a media key, the one-way function combines the media key with a nonce generated by a number generator to produce a bus key and the encryption logic encrypts the data accessed from the storage medium using the bus key prior to transmitting the encrypted data via a data bus. Accordingly, Applicant respectfully submits that Claim 18 is not obvious over Natsume in view of Miyauchi and requests withdrawal of this rejection.

For all the foregoing reasons, it is respectfully submitted that independent Claims 1, 11 and 18 are in condition for allowance. Regarding dependent Claims 2-10, 12-17 and 19-26, Applicant submits that these claims are not obvious in view of the cited references at least for the same reasons given in connection with their base Claims 1, 11 and 18.

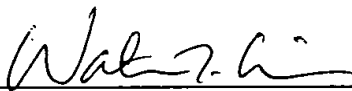
### CONCLUSION

In view of the foregoing, it is believed that all claims now pending patentably define the subject invention over the prior art of record and are in condition for allowance, and such action is earnestly solicited at the earliest possible date. If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees. If a telephone interview would expedite the prosecution of this Application, the Examiner is invited to contact the undersigned at (310) 207-3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

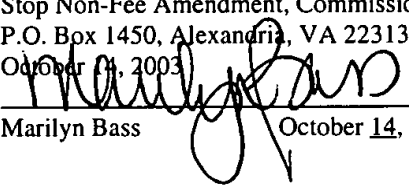
Dated: October 14, 2003

  
\_\_\_\_\_  
Walter T. Kim, Reg. No. 42,731

12400 Wilshire Boulevard  
Seventh Floor  
Los Angeles, California 90025  
(310) 207-3800

#### **CERTIFICATE OF MAILING:**

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail , with sufficient postage, in an envelope addressed to: Mail Stop Non-Fee Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on  
October 14, 2003

  
\_\_\_\_\_  
Marilyn Bass

October 14, 2003